United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

INFORMATION WARFARE: ISSUES ASSOCIATED WITH THE DEFENSE OF DOD COMPUTERS AND COMPUTER NETWORKS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
LCDR DEREK L. FRANKLIN, USN

AY 01-02

Mentor: Dr. Donald F. Bittner, Professor of History
Approved: ______________________
Date: ______________________

Mentor: Lieutenant Colonel Charles L. Hudson, USMC
Approved: ______________________
Date: ______________________

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burder for this collection of information is estibated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burder to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 12-04-2002	2. REPORT TYPE Student research paper	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2002

4. TITLE AND SUBTITLE Information Warfare: Issues Associated with the Defense of DOD Computers and Computer Networks Unclassified	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Franklin, Derek L. ;	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS USMC Command and Staff College 2076 South Street MCCDC Quantico, VA22134-5068	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS USMC Command and Staff College 2076 South Street MCCDC Quantico, VA22134-5068	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 63	19. NAME OF RESPONSIBLE PERSON EM114, (blank) lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. AGENCY USE ONLY (LEAVE BLANK)

2. REPORT DATE
12 APRIL 2002

3. REPORT TYPE AND DATES COVERED
STUDENT RESEARCH PAPER – 1 OCT 01 TO 12 APR 2002

4. TITLE AND SUBTITLE

INFORMATION WARFARE: ISSUES ASSOCIATED WITH THE DEFENSE OF DOD COMPUTERS AND COMPUTER NETWORKS

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)
Lieutenant Commander Derek L. Franklin, USN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC COMMAND AND STAFF COLLEGE
2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER

NONE

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SAME AS #7.

10. SPONSORING/MONITORING AGENCY REPORT NUMBER:

NONE

11. SUPPLEMENTARY NOTES

NONE

12A. DISTRIBUTION/AVAILABILITY STATEMENT

CLEARED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED.

12B. DISTRIBUTION CODE

N/A

13. ABSTRACT *(MAXIMUM 200 WORDS)*

The threat to the Defense Information Infrastructure is growing. Hackers have advanced in sophistication and the potential exists for an alliance of independent hackers and terrorist/criminal groups that may threaten the critical information pathways of the armed forces. An analysis of the history of computer information warfare reveals that there was an embarrassing lack of readiness and defense capability available to the armed forces of the United States before 1999. With the establishment of the Joint Task Force-Computer Network Defense (JTF-CND), later renamed to Computer Network Operations in 1998 (JTF-CNO), a minimum capacity to respond has been developed. However, as the issue has grown in importance, policy makers and planners have come to realize the limitations of Computer Network Attack (CNA) and Computer Network Defense (CND) as warfare areas. The growth of related legal and law enforcement issues, and the effect of a possible enemy CNA strike, will require the coordination of civilian, armed forces, and law enforcement officials to respond effectively. This will prevent CNA/CND from being a purely military issue.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)

Computers, Computer Network Attack, Computer Network Defense, Computer Network Operations, Network Centric Warfare, Information Warfare

15. NUMBER OF PAGES:
53

16. PRICE CODE: **N/A**

17. SECURITY CLASSIFICATION OF REPORT

UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE:

UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT

UNCLASSIFIED

20. LIMITATION OF ABSTRACT

/

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCUDE THE FOREGOING STATEMENT. QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Executive Summary

Title: INFORMATION WARFARE: ISSUES ASSOCIATED WITH THE DEFENSE OF DOD COMPUTERS AND COMPUTER NETWORKS

Author: Lieutenant Commander Derek L. Franklin, United States Navy

Thesis: The threat to the Defense Information Infrastructure (DII) is growing. Hackers have advanced in sophistication and the potential exists for an alliance of independent hackers and terrorist/criminal groups that may threaten the critical information pathways of the armed forces. An analysis of the history of computer information warfare reveals that there was an embarrassing lack of readiness and defensive capability available to the armed forces of the United States prior to 1999. With the establishment of the Joint Task Force-Computer Network Defense (JTF-CND), later re-named Joint Task Force- Computer Network Operations (JTF-CNO), a minimum capacity to respond has been developed. However, as the issue has grown in importance, policy makers and planners have come to realize the limitations of Computer Network Attack (CNA) and Computer Network Defense (CND) as warfare areas. The growth of related legal and law enforcement issues, and the effect of possible enemy CNA strikes, will require the coordination of civilian, armed forces, and law enforcement officials. This will thus prevent CNA/CND from being a purely military issue.

Discussion: Although the Internet is more than three decades old, it is only in the last five to seven years that senior government officials have given serious thought to the vulnerability of DOD computer networks and computers systems. Meanwhile, potential adversaries have rapidly embraced information technology and computer network attack as force multipliers that can weaken or exploit critical vulnerabilities of a larger adversary's information infrastructure. In response to Joint Vision 2010 and its emphasis on information dominance, as well as several highly publicized network intrusions, the JTF-CND (later JTF-CNO) was established in 1998.

When a sophisticated hacking campaign directed at sensitive U. S. computers was detected in 1999, serious questions arose concerning the integrity of DOD unclassified and classified computer networks, and the dependability of the commercial communications infrastructure on which DOD depends. DOD began to commit substantial resources to the protection effort. Despite efforts to share information and develop common operating procedure, confusion remains regarding authority and responsibility. The GAO recently concluded in late 2001 that despite the resources devoted to the network defense mission, as a whole the Federal government is only marginally better at defending its computers and computer networks than it was five years ago.

Conclusion: Although the nation as a whole, and the armed forces specifically, are better prepared than in 1998 to detect and blunt the effects of a computer attack, the potential damage an attack could cause may still be catastrophic, although this would still be less than a kinetic attack. However, in order to use the full capability of CNA/CND many legal issues must be resolved (both domestically and internationally). U.S.

constitutional and privacy issues must be resolved and international agreements must be established delineating appropriate use of computer attack and defense resources. As potential adversaries gain more experience and have more sophisticated tools at their disposal (at an ever-cheaper price), DOD will be hard-pressed to counter the threat.

Table of Contents

Illustrations

Tables

Preface

In 1998, after returning from an overseas assignment, I was assigned to the Defense Information Systems Agency (DISA) in Arlington, VA. After a few months as a program/budget analyst, I was then attached to a fledgling new organization: the Joint Task Force-Computer Network Defense (JTF-CND) to fill the J1/4/8 (Personnel/Logistics/Resources) chief billet. In this capacity, I had the pleasure of working directly for the commander, Major General (as of this writing Lieutenant General) John H. Campbell, United States Air Force, who also wore another hat as the Vice-Director of DISA.

My experience with the task force was transformative. As a senior US Navy lieutenant, I was responsible for a multimillion-dollar budget and working with senior officers in a fast paced joint environment that seemed more being part of a frontier town than anything else. For the first time, I was exposed to a high technology, computer intensive environment that was judged by some to be a new and transformational type of warfare. Each day was, by turns, exhilarating and humbling. Not only was I the entire staff of the J1/4/8 (J6-C4I/Information Technology responsibilities were later added to my portfolio), but I continued to be amazed as I learned more about the massive information technology infrastructure that allowed the US armed forces to efficiently conduct global operations.

Today, the JTF-CNO has matured. The missions of computer network attack and computer network defense now have a higher profile that is reflected by the assignment of these missions in the Unified Command Plan of 1999 to the Commander-in-Chief, Space Command, headquartered in Colorado Springs, Colorado. From an initial cadre of 18 armed forces and civilian staff members in 1998, the current organization is projected to grow to nearly 150 staff members. The current (April 2002) JTF-CNO commander is Major General James D. Bryan, United States Army. The constant continues to be the highly professional and proficient civil service civilians, military personnel, and private contractors who labor in anonymity to defend Department of Defense computers and computer networks. I have been proud to be associated with them.

No preface would be complete without my acknowledgement of the debt I owe to numerous individuals in the preparation of this work. They include several members of the JTF-CNO (too numerous to name) who generously gave of their time and expertise to review this work. I am also especially appreciative to my faculty mentors at the U. S. Marine Corps Command and Staff College, Dr. Donald F. Bittner, Ph.D. and Lieutenant Colonel Charles L. Hudson, USMC. I am grateful to all for their patience, encouragement, expertise, goodwill, and occasional forceful prodding. The success of this work is due to all of these professionals; any mistakes that remain are mine and mine alone.

Finally, I wish to thank my family, my wife Cecilia, my daughters Leslie and Marguerite, and my son, Miles for their patience and understanding. With their support I have been able to overcome and achieve, without them success and accomplishment are meaningless.

DEREK L. FRANKLIN
Lieutenant Commander, USN
Quantico, VA
April 2002

The New Battlefield

In 1999, two pieces of information appeared in the U.S. press and attracted little attention. The first was a report on a heretofore-secret government investigation to determine the source or sources of intrusions into sensitive US government computers. The operation was named "Moonlight Maze." The attacks were believed to have originated from Russian government offices and speculation was rampant as to how long the intrusions had been occurring, whether the computer probes were government sponsored in nature, and whether sensitive or classified material may have been accessed by the hackers.[1]

In February of the same year, two Chinese Air Force Colonels, Qiao Liang and Wang Xiangsui, published *Unrestricted Warfare*. That it appeared at all in Beijing is indicative of government approval. It is believed to be intended as a primer for young officers on the various types of warfare that China will be involved in the new century. Although translations of the work were slow in being disseminated, armed forces intelligence officials in the United States are alarmed by the work's matter-of-fact emphasis on using the Internet and computer networks as a force multiplier to cripple an enemy's infrastructure. Among the authors' comments:

> If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus

[1] Anthony Kimery, "Moonlight Maze ," Infowar, 3 December 1999, URL: http://www.infowar.com/class_2/99/class2_120399b_J.shtml. Accessed 14 January 2002. Hereafter cited as Kimery, Moonlight Maze.

> and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis.[2]

A report delivered to Congress in November 2001 was particularly disturbing in its candid assessment of the federal government's computer vulnerabilities. The Government Accounting Office (GAO) report, delivered nearly two months after the September 11, 2001 terrorist attacks in the United States, concluded:

> Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations.[3]

The obvious conclusion to be drawn from these reports is that the federal government and the Department of Defense, in particular, remain vulnerable to outside attack and exploitation of computers and computer networks at the dawn of the 21st century. Indeed, despite early identification of the critical vulnerabilities and the best efforts of hundreds, perhaps thousands, of armed forces personnel, government civilians, and defense contractors, DOD would appear to be only marginally better protected than

[2] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, 1999), 145-146. A complete text of this work is available at: URL: <http://www.terrorism.com/documents/unrestricted.pdf>

[3] General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets* (Washington DC: GPO, 2001), 6.

when it began to examine the issue of protecting its critical vulnerability infrastructure in 1997.

At the dawn of the 21st century, the United States finds itself under attack on several fronts from enemies that are diverse in their membership, geographically dispersed, and technologically sophisticated. Moreover, these adversaries are motivated by several factors. These include greed, political and religious ideology, and emotional fanaticism. These foes vary in their complexity. The threat may be as innocuous as a teenager hacking into a government computer system to impress fellow hackers or as serious as a friendly state sponsoring teams of sophisticated hackers to conduct "data-mining" operations to gain military information with a possible use of such knowledge against the US in the future. Furthermore, the last few years have also seen the emergence of cyberspace guns for hire; these are individuals and teams who hire their services to the highest bidder and whose targets are unclear.[4]

The US government responses to computer threats to its critical infrastructure will vary widely. This depends on the source and nationality of the attackers, whether US laws have been broken, and the actual damage sustained. It is a tedious business, complicated by multilayered bureaucracies, domestic and international legal ramifications, and the necessity to achieve a high degree of confidence that the act is correctly attributed to an identifiable person or organization.

[4] J.R. Wilson, "Cyberwarfare 101," URL: <www.mit-kmi.com/Archives/5_1_MIT/5_1Art4.cfm>. Accessed 31 December 2001. Hereafter cited as Wilson, Cyberwarfare online article. In this article, Wilson describes the variety of hackers that proliferate in the hacking community. They cut across every demographic in terms of age, education, and motivation. However, the vast majority of "problem" hackers that concern DOD are young and easily manipulated. Furthermore, with the profusion of more sophisticated tools available to more people, the sophistication level of hackers is dropping. Few hackers now know how to write computer code, for example.

While the JTF-CNO is not the only organization working these issues, it is the lead organization within the DOD for computer network defense and computer network attack. As such, it is the trigger-puller for this new branch of warfare. It is the pathfinder organization for DOD computer network security, yet few have heard of it and fewer still understand its mission.

Historical Perspective

In July 1996, the Chairman of the Joint Chiefs of Staff, Army General John M. Shalikashvilli, published *Joint Vision 2010* (hereafter referred to *as JV 2010*). In it, and its follow on publication *Joint Vision 2020*, the concept of full spectrum dominance across the complete range of armed forces operations was promulgated.[5] *JV 2010* identified information technology superiority as a prerequisite for full spectrum dominance. *JV 2010* also assumed that gaining and maintaining this advantage would require defensive as well as offensive capability.[6] However, in 1996, the bold words in *JV 2010* did not match the reality of how CINCs, services, and agencies operated. Even as *JV 2010* was distributed, senior armed forces theorists and policy makers recognized that it had only shone a small light on an enormous problem. There was still much to learn about the scope of the task at hand, and the next two years provided impetus to the work that lay ahead.

Despite the spate of Internet e-mail viruses over the last few years, as early as 1985 viruses had already appeared and demonstrated how a relatively small amount of unsophisticated computer code could cripple an individual computer or computer network. From six viruses that had been identified in 1987, by mid-2001 the figure had grown to thousands of viruses and many more thousands of variants. In recognition of the potential impact that interruption of the nation’s information infrastructure could have on business and government operations, in July 1996, the Clinton administration issued

[5] Joint Staff, *Joint Vision 2010* (Washington DC: GPO, 1996), 2.

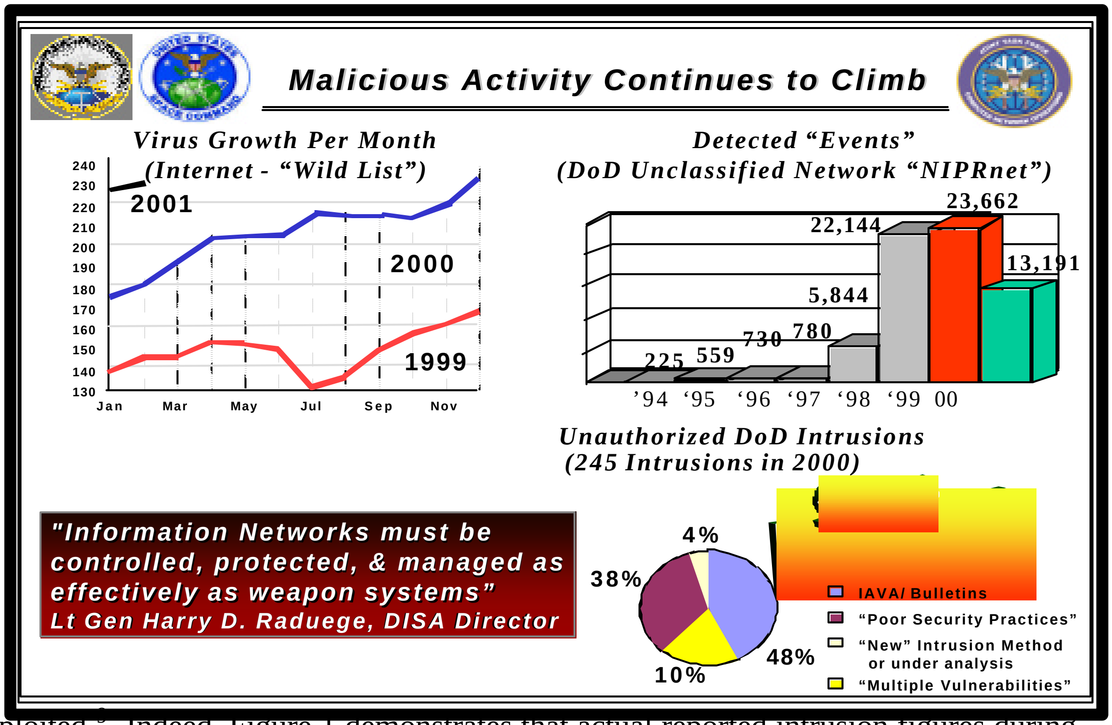
Executive Order 13010.[7] This order established the President's Commission on Critical Infrastructure Protection (PCCIP). Although the commission's focus was a national information infrastructure vulnerability assessment, it was also tasked with establishing a national attack warning capability. This was the recommendation that brought DOD into this arena.

To fulfill the charge of establishing a national attack warning capability, an assessment of existing vulnerabilities was necessary. In June 1997, in the wake of *JV 2010* and the establishment of the PCCIP, computer experts from the highly secretive National Security Agency (NSA) were assigned the task of breaking into DOD computers and computer networks, as well as other vulnerable targets in other Federal agencies. Using easily obtainable software and hardware, the "red cell" would have been able to wreck havoc on computers and networks throughout the Federal government.[8] The exercise, dubbed ELIGIBLE RECEIVER, shattered existing illusions about the security of United States information technology infrastructure. Over 60% of the U.S. government systems probed during the exercise were discovered to have security holes that could be easily

[6] Joint Staff, *Joint Vision 2010*, 20.

[7] U.S. President, Executive Order 13010, "Critical Infrastructure Protection," 15 July 1996. A copy may be found at the National Archive and Records Administration site, URL: http://www.nara.gov/fedreg/eo1996.html. Accessed 12 April 2002.

[8] A red cell is a group organized to test the effectiveness and security of an organization's defenses. In the case of the NSA red cell, the team was prohibited from causing real damage and was refereed in their efforts. For additional information on the ELIGIBLE RECEIVER red cell see: Bill Gertz, "Eligible Receiver," *Washington Times*, 16 April 1998.



"Information Networks must be controlled, protected, & managed as effectively as weapon systems"
Lt Gen Harry D. Raduege, DISA Director

exploited.[9] Indeed, Figure 1 demonstrates that actual reported intrusion figures during this time were also rising despite the increased monitoring of DOD networks.

Figure 1. Malicious Activity Continues to Climb. Source: JTF-CNO, JTF-CNO Operations Brief, May 2001.[10]

Another equally disturbing discovery appeared: no one individual or agency had authority or responsibility for coordinating computer network defense response for the Federal government, including DOD. Despite the fact that most governmental agencies

[9] Drawn from text of Command, Control, Communication, Computers, and Intelligence Surveillance Reconnaissance online forum (C4ISR) incorporated in "Eligible Receiver Exercise Shows Vulnerability," Infowar.com, 22 December 1997, URL: <http://www.infowar.com/civil_de/civil_022698b.html-ssi>. Accessed 15 January 2002.

[10] Brief has not been previously published. Brief available from Operations directorate (J3) of the Joint Task Force-Computer Network Operations (JTF-CNO), co-located in the Defense Information Systems Agency (DISA) headquarters building in Arlington, VA.

[11] Drawn from text of Command, Control, Communication, Computers, and Intelligence Surveillance Reconnaissance online forum (C4ISR) incorporated in "Eligible Receiver Exercise Shows Vulnerability," Infowar.com, 22 December 1997, URL: <http://www.infowar.com/civil_de/civil_022698b.html-ssi>. Accessed 15 January 2002.

had individuals in charge of information technology, training was haphazard and not standardized. Even more indicative of the problem, many system administrators (even of classified networks) did not possess the appropriate security clearance to work on the systems for which they were responsible, and there was little or no information sharing mechanisms established to promote prevention or to mitigate damage.

The press and public were slow to appreciate the importance of ELIGIBLE RECEIVER. As late as April 1998, the Assistant Secretary of Defense for Public Affairs, Kenneth H. Bacon, minimized the importance of the exercise. He benignly declared, "…ELIGIBLE RECEIVER…succeeded beyond its planner's wildest dreams in elevating…awareness of threats to our computer systems…"[12]

While the assistant secretary's comments were a slick information operation itself, in actuality, ELIGIBLE RECEIVER was an embarrassment for federal government security professionals. Even as Assistant Secretary Bacon spoke, another setback was unfolding. Since February 1998, intrusions into Pentagon and the Massachusetts Institute of Technology networks had been detected. More ominously, the origin of these intrusions appeared to originate from outside the United States. Contrary to the *modus operandi* used by most amateur hackers, the purpose was not to simply deface a web site and leave telltale Internet "graffiti." Rather, the objective was to probe these sites and to

[12] Kenneth H. Bacon, "DOD News Briefing with Assistant Secretary of Defense (Public Affairs)," press conference available at URL: <http://www.defenselink.mil/news/Apr1998/t04161996_t0416asd.html>, 16 April 1998. Accessed 14 January 2002

download information.[13] The hackers collected numerous passwords and planted "backdoors" to use to return to the networks undetected.[14]

The subsequent investigation brought together resources from five federal agencies[15] and approximately 30 agents from the Federal Bureau of Investigation.[16] The perpetrators were identified as two Northern California teenagers and their Israeli based mentor, an eighteen-year-old hacker named Ehud Tenebaum (who preferred his online moniker of Analyzer). Before he was caught, Tenebaum bragged about breaking into over 1,000 Internet servers and establishing 120,000 computer user accounts on them.[17] Establishment of these accounts would allow the hackers numerous avenues to access the servers through what the computer system would assume to be valid accounts. The Justice Department, in cooperation with the Israeli government, arrested all three of the suspects. Still, this incident revealed United States vulnerability to even unsophisticated hacking. Three young hackers, all self-taught, were able to easily access sensitive

[13] Virginia Key "What is Solar Sunrise," URL: <www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm>, Date unknown. Accessed on 13 January 2002. Hereafter cited as Key, Solar Sunrise.

[14] In computer parlance, backdoors are software computer vulnerabilities that allow programmers to reenter software programs and networks while bypassing normal security measures such as passwords and limited access. While backdoors have a legitimate use for people such as system administrators, the term has become synonymous with hackers who are intent on using the backdoors to disrupt computer networks.

[15] The five agencies were Department of Justice and its subordinate agency the Federal Bureau of Investigation, Air Force Office of Special Investigation, National Aeronautic and Space Administration, and the Naval Criminal Investigative Service. For more information see: Department of Justice press release, "Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers," found at URL: <http://www.usdoj.gov/criminal/cybercrime/ehudpr.htm>, 18 March 1999. Accessed 10 January 2002.

[16] Key, Solar Sunrise.

[17] Key, Solar Sunrise. Tenebaum boast must be viewed skeptically. An FBI profile of young hackers and their culture indicated that such boastfulness was a common characteristic.

information. Although MIT and DOD would both claim that the information was not classified, skepticism remains.

In May 1998, in part influenced by the events of the previous two years (including recommendations of the PCCIP[18] and lessons learned from ELIGIBLE RECEIVER), President Clinton issued a Presidential Decision Direction (PDD), No. 63.[19] Although the directive contained many important initiatives, four were most significant:

1. Establishment of a national center to warn of and respond to attacks.

2. Requirement for the entire federal government to reduce exposure to new threats.

3. Establishment of an office of a national coordinator for infrastructure protection.

4. Establishment of the National Infrastructure Protection Center (NIPC) at the FBI to fuse governmental resources and to coordinate responses to attacks across the Federal government.[20]

Spurred by the PCCIP report, the Secretary of Defense (SECDEF) agreed that the time had come to create a single organization responsible for "…coordinating and

[18] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997, 93-99.

[19] Presidential Decision Directive NSC 63, *Critical Infrastructure Protection*, 22 May 1998. Full text available at Federation of American Scientists website, URL: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. Accessed 12 April 2002.

[20] It is worth noting that the NIPC was organized and modeled after the Centers for Disease Control and Prevention. This is logical, given the medical analogies used in connection with computer networks such as concepts of viruses, infection, and containment. See: Michael Tompkins, "Computer Network Defense at the National Level," URL: <http://rrsans.org/country/defense.php>, 5 December 2000. Accessed 14 January 2002.

directing the defense of DOD computer systems and computer networks…"[21] However, before DOD could fully man the new Joint Task Force-Computer Network Defense organization, it had to contend with an operation known as Moonlight Maze.

Moonlight Maze was the title given to the investigation of Russian intrusions into U.S. government computers and networks. These intrusions were first detected in January 1999 and continued until June of that year. Although no individual was charged with any crime and the intrusions are believed to have stopped, the investigation is still ongoing (under a different codename). The two major unanswered questions from the investigation remain: was the hacking state sponsored, and was the DOD classified information network compromised?[22]

However, equally important to the Clinton administration officials was that Moonlight Maze represented a quantum leap in sophistication from previous attacks. Furthermore, the possibility that a sovereign nation was engaged in this activity revealed numerous flaws in the government's approach towards computer network defense.

Ultimately, Moonlight Maze raised more questions than it answered. Still undetermined was the question of how does the United States apportion, with a high

[21] Secretary of Defense (William S. Cohen), letter to CINCs, services and agencies, subject: "Joint Task Force-Computer Network Defense Charter," 4 December 1998. Cited hereafter as Cohen Charter.

[22] The U.S. armed forces have two primary computer networks that it relies upon to conduct day-to-day business. The first is the Non-classified Internet Protection Router Network or NIPRNET. The second is the Secret Internet Protection Router Network of SIPRNET. NIPRNET is DOD's worldwide unclassified network. While the network is a separate entity, connectivity is achieved by "riding" on the World Wide Web (or Internet) infrastructure. This means that this information is susceptible to outside manipulation and attack, and has little inherent security. In the early days of computer networking, it was even possible to reach the SIPRNET through numerous special access gateways in NIPRNET. These gateways have since been identified and shut down and the SIPRNET is now a completely separate and encrypted network. While no U. S. government official has gone on record to admit to SIPRNET compromise, some observers believe otherwise. Kimery, Moonlight Maze.

degree of certainty, responsibility for an intrusion? If the responsible party is a nation, what recourse is available? As of 1999, few countries had laws criminalizing hacking. In fact, the laws around the globe had not caught up with technological advances. Many nations did not make hacking a crime; for example, hacking in Russia was not a crime when the Moonlight Maze intrusion was discovered. In the absence of legal restrictions, all the US could do upon discovery of the Moonlight Maze intruder(s) was to send a diplomatic letter of protest.[23]

Moonlight Maze revealed just how impotent the DOD could be against a determined adversary. Nevertheless, even as technicians and analysts were compiling their after action reports, changes were underway that would reshape the DOD response to future threats. The answer lay in building a new organization with the punch to protect and perhaps to one day take offensive action to protect the DOD information infrastructure.

[23] Kimery, Moonlight Maze.

Mission/Organization

In December 1998, the Joint Task Force-Computer Network Defense (JTF-CND) was established.[24] A cadre of 18 full time civilian and armed forces staff members were assigned to it and the unit was tasked to achieve final operating capability by 30 June 1999. From the beginning, the organization was intended to be a stopgap measure until the Unified Command Plan process could address CINC responsibility for the mission.[25]

The initial focus of the organization was DOD computer network defense with the joint task force reporting to the SECDEF. After approval of the Unified Command Plan (UCP) in 1999, JTF-CND reported to CINC, Space Command (CINCSPACE), a four star Air Force officer headquartered in Colorado Springs, Colorado. Over time, the CND relationships (depicted in Figure 2) became formalized and continue to exist today. In April 2001, JTF-CND was renamed the Joint Task Force-Computer Network Operations or JTF-CNO.[26]

From this basic beginning, the mission of the task force has evolved. While the initial focus of effort was computer network defense, over time advances in technology made computer network attack (CNA) a viable mission. However, CNA remains a

[24] Cohen Charter, 6-10.

[25] The Unified Command Plan allocates responsibilities among the nine combatant commands. It establishes these commands' missions, responsibilities, and force structure. The plan also defines the geographical commands' areas of responsibilities. Taken from URL: <http://www.defenselink.mil/specials/unified>. Accessed 14 January 2002.

sensitive mission and its employment requires SECDEF or higher approval for legal reasons (see pages 25-36, legal section, of this paper). Nevertheless, the CNO mission can be explained in the following context:

Computer Network Operations (CNO) Responsibilities	
Computer Network Attack (CNA)	***Computer Network Defense (CND)***
• Coordinator for CNA requirements, development and employment across CINCs, services, and agencies • Provide CNA support to Unified commanders via USSPACECOM as supporting CINC • Conduct CNA Ops (trigger pullers) • Intelligence/Counterintelligence	• Defend DOD networks from intrusion • Coordinate DOD response to intrusions and attack across DOD • Law Enforcement Coordination • Intelligence/Counterintelligence • Technical Analysis

Table 1. CNO Responsibilities (Source: JTF-CND Charter and JTF-CNO Concept of Operations)[27]

The JTF-CNO has five components drawn from each branch of the armed forces and from DISA. These include:

[26] The JTF-CND became the JTF-CNO on 2 April 2001. USCINCSPACE letter to Commander, Joint Task Force-Computer Network Operations and others, subject: "Redesignation of Joint Task Force-Computer Network Defense," 23 March 2001. Copies held at USCINCSPACE and JTF-CNO.

[27] Cohen Charter, 2-7; also USSPACECOM document, subject: "JTF-CNO Concept of Operations." 12 April 2001

- **ACERT** (Army Computer Emergency Response Team) a part of LIWA (Land Information Warfare Activity), located at Fort Belvoir, VA

- **AFCERT** (Air Force Computer Emergency Response Team): 67th IW at Lackland AFB, Texas

- **NAVCERT** (Navy Computer Emergency Response Team): Navy Component Task Force for Computer Network Defense (NCTF-CND), located in Washington, D.C.

- **MAR-CND** (Marine Corps Forces-Computer Network Defense): MIDAS (Marine Intrusion Detection Analysis System) at Quantico, VA.

- **DOD-CERT**: Support provided through the Global Network Operations Center (GNOSC) located in Arlington, VA.

All components report to JTF-CND/CNO for tactical matters (i.e., the JTF-CNO commander has tactical control or TACON of these subordinate units). However, these components also play a dual role as the CERTs (Computer Emergency Response Teams) for their services as well as reporting to the respective service or agency for all other operational and administrative matters. None of the components employs CNA capabilities. The CNA "toolkit" resides in the JTF-CNO Operations directorate (J3) and is offered to the supported CINC by USSPACECOM. Decisions to employ CNA capability rests with the Secretary of Defense and the President.

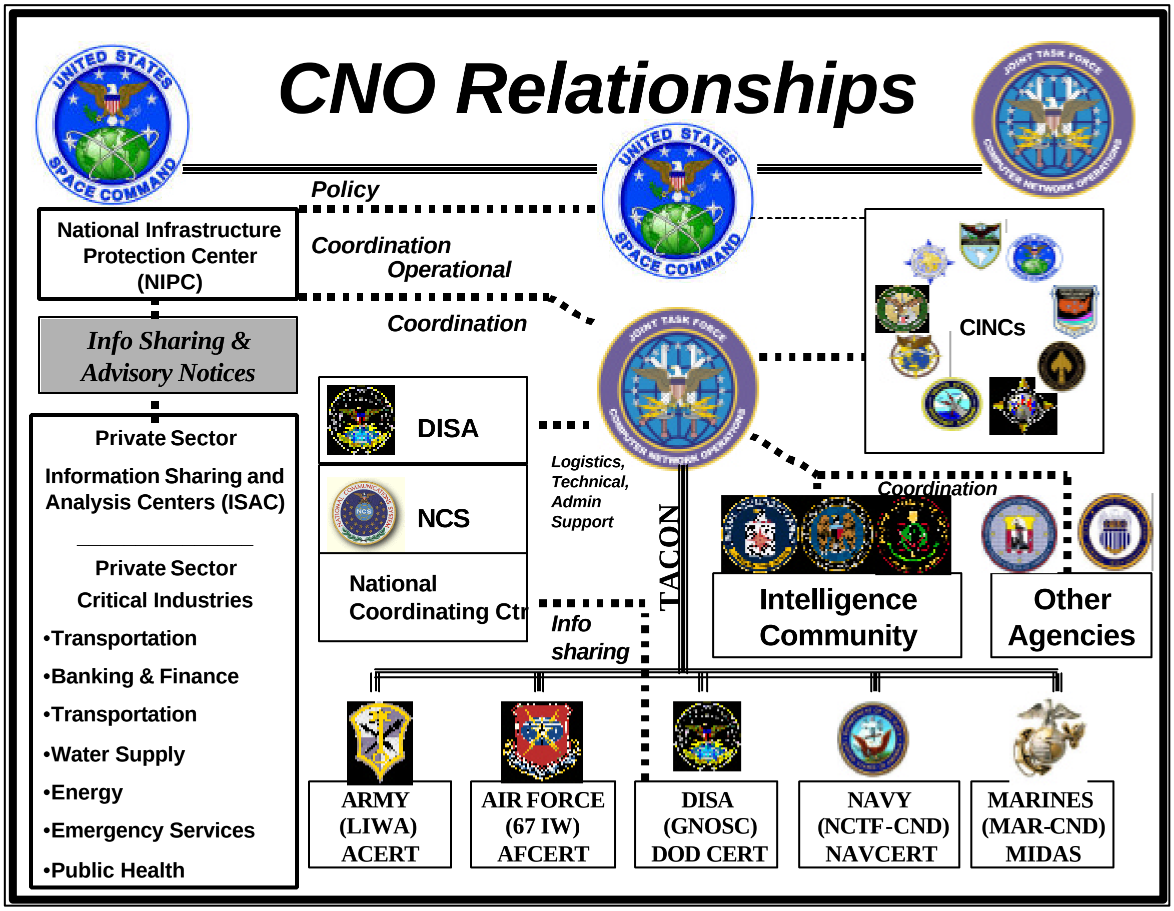


Figure 2. CNO Relationships. Source: JTF-CNO Command Brief, Nov 2001.[28]

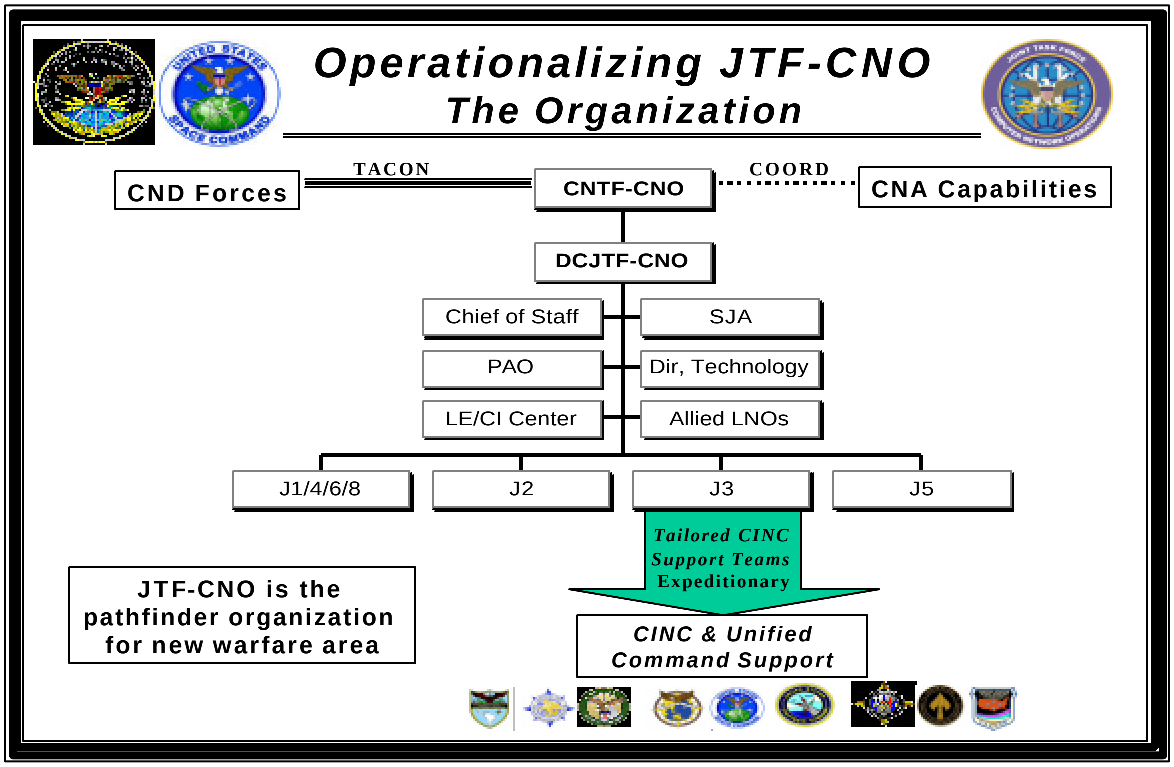
As the single DOD point of contact for CND and CNA, JTF-CNO is the armed forces equivalent to the FBI's NIPC. It is important to reiterate that JTF-CNO has no responsibility for protecting any computers or computer networks outside DOD. However, given the overlaps between commercial, federal government, and DOD infrastructures, it should be no surprise that the task force is involved in information

[28] Original brief previously unpublished. Briefing is currently held in Operation Directorate (J-3) of the Joint Task Force-Computer Network Operations, which is co-located at the Defense Information Systems Agency headquarters in Arlington, VA.

sharing at all levels and across all bureaucratic boundaries and maintains an active liaison function. Coordination also exists between the JTF-CNO, the intelligence community, and DOD law enforcement agencies for tactical and operational matters. Currently based in Arlington, VA, the JTF-CNO is a vibrant and growing organization that is expected to grow to 144 staff members by the end of fiscal year 2002 (30 September 2002).[29]

As currently organized, the JTF-CNO looks like most joint US armed forces organizations. The commander is a two-star military officer who is dual-hatted as the Vice Director of the Defense Information Systems Agency. In his JTF role, he has tactical control of the organizations depicted in Figure 2. The deputy commander (DCJTF-CNO), currently a one-star Navy officer as depicted in Figure 3 assists the JTF-CNO commander in his duties. Senior advisors include a chief of staff, director of technology, staff judge advocate, and public affairs officer. However, the organization also has twelve permanent liaison officers that are assigned from the Defense Intelligence Agency (DIA), National Security Agency (NSA), Air Force Office of Special Investigation (AFOSI), Naval Criminal Investigative Service (NCIS), and the Army Criminal Investigative Division (CID). The organizational structure also provides for eventual assignment of Allied liaison officers. Although these Allied billets are currently unfilled, it is expected that traditionally close allies, such as the United Kingdom and Australia, will likely be the first foreign representatives. Others may be added at a future date.

[29] Joint Task Force – Computer Network Operations "JTF-CNO (Command Brief) November 2001.



Operationalizing JTF-CNO

The Organization

CND Forces

TACON

CNTF-CNO

COORD

CNA Capabilities

DCJTF-CNO

Chief of Staff

SJA

PAO

Dir, Technology

LE/CI Center

Allied LNOs

J1/4/6/8

J2

J3

J5

Tailored CINC Support Teams Expeditionary

CINC & Unified Command Support

JTF-CNO is the pathfinder organization for new warfare area

Figure 3. JTF-CNO Organization. Source: JTF-CNO "Command Brief" 1 November 2001.

All of this organizational structure and inherent capability, including hardware, software, facilities improvement, contractor support, etc., will come at a significant cost. Original estimates were that the JTF-CNO would need a budgetary increase from 3.1 million dollars in fiscal year 2000 to between 18-25 million dollars by fiscal year 2003.[30] A large amount of this increase would be devoted to facilities and technology upgrades, investments in the private sector for developing new CND and CNA tools, and hiring contractors.

[30] Joint Task Force –Computer Network Defense "CINC Decision Brief" 28 February 2001.

It is worthwhile to note that the JTF-CNO is not the only organization where CND activity takes place. At an elementary level, each user who uses standard security practices and each system administrator who implements updates to virus software is engaging in CND activity. But, while CND and CNA are elements of information operations, it is crucial to understand that these are the JTF-CNO's only missions and that they are the only organization charged with CND and CNA responsibility across DOD.

Other DOD-wide missions related to other information operations such as psychological operations and electronic warfare fall under the purview of the Joint Information Operations Center (JIOC) headquartered at Kelly Air Force Base in San Antonio, Texas.[31] That command also reports to CINCUSSPACECOM. An operational framework is in place to allow warfighting consumers to do one-stop shopping for IO and each command is organized with "away teams" that travel to the supported CINC and can offer a variety of IO services. While not officially designated as the information operations "czar," USSPACECOM is as close as any organization to being an overall coordinator for the military services.

While the non-CND/CNA information operations capability of the JIOC and similar organizations throughout DOD deserve further study, the scope of such research is beyond the focus of this work. As the CND and CNA designated DOD "trigger-pullers" for this new warfare area, the JTF-CNO will be the organization that will be examined in detail throughout this work.

[31] While CNA and CND are elements of information operations (IO), there is a broader spectrum of IO tasks that include psychological operations, civil and public affairs, electronic warfare, military deception, and operational security. Because of the legal ramification of CNA, DOD has keep the CNA and CND mission areas separate from the broader group of IO tasks.

CNA Threats: Fact versus Fiction

There may be those who still believe that information warfare in cyberspace is still some years away. In fact, on at least two occasions the United States has used information warfare to influence operations on the battlefield. During 1991 in the midst of the Persian Gulf War, e-mail used by Iraqi commanders was intercepted. While the practical effect was minimal and did not decisively influence the conduct of the war, nevertheless the episode demonstrated the potential for information operations conducted in cyberspace.[32] The second serious attempt at computer information operations occurred in 1998 during the Kosovo air campaign. In this conflict, the effectiveness of Yugoslavia's air defense network was undermined by the manipulation of the interconnected computers of the system. Deceptive messages and false targets were inserted to deceive the enemy.[33]

Similar attempts to influence the enemy's perception of the battlefield litter the historical record. During World War II, numerous examples of information operations can be cited, the most elaborate and perhaps most famous of which were the numerous deception operations undertaken in support of the June 1944 Normandy landings.[34]

[32] David A. Fulghum and Robert Wall "Combat-Proven Infowar Remains Underfunded," *Aviation Week & Space Technology*, 26 February 2001, 52.

[33] Fulghum and Wall, 52.

[34] The planners of the Normandy invasion went to great lengths to integrate deception operations into the invasion planning. Since the Germans were certain the aggressive U.S. Army officer General George S. Patton would lead the invasion, Allied planners created the fictitious First U.S. Army Group (FUSAG) and made sure that the Germans were fed a stream of data that they could verify through Germany's spy

While technology has advanced since these early attempts of the last decade, caution must be used in order not to overstate what is possible in the realm of computer information warfare. Scenarios of hackers taking over nuclear launch capability are far-fetched fiction; one JTF-CNO official, Commander Robert Gourley, formerly the J2 (Intelligence Officer) of JTF-CNO, believes that, for the foreseeable future cyber weapons will not come close to the destructive potential of conventional kinetic weapons and certainly will not approach the destructive power of nuclear weapons. Gourley has stated:

> It is easy to overestimate the capabilities of computer network attacks. I don't think we will ever reach the stage where you could bring down an entire society with cyberattack. If properly executed, such an attack could cause trillions of dollars of damage to an economy and even kill people by crashing airlines, for example, but that is not a threat to completely destroying our economy. The only threat to our society I've seen on that scale is a nuclear attack.[35]

If this assessment is correct, then why the concern and focus on cyber war? The answer lies in the number and origin of potential threats. While the single, ubiquitous hacker is still perceived as a serious but manageable threat by Gourley and the JTF-CNO, hackers of all types have increased their individual capability through hacker tools easily downloaded from the Internet and have begun to cooperate with virus writers (a different

network. Ultimately, the plan convinced Hitler of the Allies intention to land a Calais and thus Hitler keep in reserve forces to repel what he believed was the true landing in force at Calais. This error is credited with buying the Allies enough time to establish a foothold ashore. One resource for more information (along with some of Patton's more colorful language) may be found at the Patton Museum of Cavalry and Armor website, URL: http://knox-www.army.mil/museum/pattonsp.htm, accessed 29 April 2002.

[35] Wilson, Cyberwarfare online article.

subset of the hacker culture). There is even some evidence to suggest alliances are developing between independent hackers and criminal/terrorist organizations.[36]

Since the terrorists' attacks of September 2001, those working in the world of computer network operations have experienced an uneasy lull. Some organizations have even had the first drop in computer security incidents since the tracking of such incidents began. In addition, a wave of attacks expected as retaliation after the start of the bombing in Afghanistan never materialized.[37]

Nevertheless, analysts familiar with the capabilities of cyber-terrorist organizations and individuals continue to believe a serious and widely scaled attack continues to be only a matter of time. The *Information Assurance Newsletter* recently published a list of the most plausible threats. These include:

- Cyber terrorists hack into international banking networks, resulting in a global loss of confidence in the financial system and significant financial losses.
- Computer network attacks disrupt trading in the major stock markets. Huge financial losses and plunging investor confidence ensue.

[36] Wilson, Cyberwarfare online article.

[37] Lisa Hoffman, "A Surprise: Fewer Cyber-Attacks after 9-11," Scripps *Howard News Service* available at URL: <www.knowstudio.com/shns/story.cfm?pk-CYBERSPACE-01-25-02&CAT-II>, accessed 26 January 2002. This article stated that the U.S. Federal Computer Incident Response Center (FEDCIRT) had recorded a nearly 50% drop in security incidents in the month after the 11 September 2001 terrorist attacks in the United States. As of January 2002, monthly incident numbers were still less than two-thirds of the expected rate. SPACECOM CINC Gen. Ralph Eberhart attributed the drop in incidents to hackers knowing "we're mad, and they're worried about repercussions."

- Disruption of air traffic control system. Public fear about safety of air travel increases. Massive losses to airline and related industries occur.
- Disruption of e-commerce through attack of Internet sites.[38]

While any of these attacks may seem daunting enough, these are not the only challenges facing the JTF-CNO. Competition for funding increased after the 11 September terror attacks amongst DOD organizations as well as other government departments. Nearly every government agency became more proactive in seeking funds to increase force protection capability, harden physical sites, decrease technology vulnerability, and, in general, raise the level of preparedness of their organizations. Many organizations, some for the first time, recognized the necessity of aggressively protecting information and ensuring connectivity throughout their units. The result has been a large increase in organizations that have a vaguely cyber-sounding name and has only added to the confusion of who is in charge government-wide for responding to potential cyber attacks.

In response to the cacophony of requirements that the White House received from throughout the government, President George Bush signed Executive Order 13231 in October 2001. The stated goal was to "ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the

[38] The Information Assurance Newsletter is a produced by IATAC (Information Assurance Technology Analysis Center) and is closely tied to the JTF-CNO and DISA. Ed Sbrocco, Tom Ward, and Chris Baden, "Cyber Terror – Potential for Mass Effect," *IA (Information Assurance) Newsletter* 4, no. 4 (Winter 2001/2002), 6.

physical assets that support such systems in the information age." Although at first blush similar to the Clinton era executive orders related to infrastructure protection, Executive Order 13231 is significant because for the first time national infrastructure, such as the banking system, telecommunications systems, and electrical grids, will now be under the same umbrella as the Defense Information Infrastructure.[39]

A key player in the order is the recently created position of Assistant to the President for Homeland Security. He or she becomes a powerful voice for federal government infrastructure protection. Issues related to protection of and recovery from computer network attacks must be coordinated with the Homeland Security office. While it is still too early to tell what effect this will have, the potential for dilution of CINCUSSPACECOM's authority and diminution of the JTF-CNO responsibility is a distinct possibility.

[39] U. S. President, Executive Order 13231, "Critical Infrastructure Protection in the Information Age," 16 October 2001. Version found in *Federal Register* 66, no 202 (18 October 2001): 53063. Hereafter cited as Executive Order 13231.

Legal Considerations[40]

As CNA and CND information warfare capabilities have matured, defense policy makers have begun to wrestle with the legal implications of cyberspace activities. Where once it may have been appropriate to use the metaphor of a wild west or gold rush town for cyberspace, a more appropriate metaphor is now that of a US territory in the late 19th century. Like a territory, the Internet has matured beyond its completely lawless stage. Order is now being imposed, albeit unevenly. However, before cyberspace matures further, questions of law and privacy must be resolved. The implications extend beyond the armed forces sphere and involve questions of international law and US constitutionality.

The JTF-CNO is very involved in this debate. One of its most important duties is to identify the source of computer attack and then to attribute it to a person, organization, and country of origin. The level of certainty will determine how the attack is to be handled. If the intrusion or attack is US based (and the offender can be identified as a US citizen), then the matter is turned over to the appropriate law enforcement agencies.[41] However, if the intruder or attacker is foreign based, then the matter is passed to the

[40] A thorough review of the legal literature related to Information Warfare is beyond the scope of this work. This section seeks to highlight only a few of the most important legal issues. For example, the Electronic Communications Privacy Act and copyright issues are not addressed. For a thorough overview of how these and other issues relate to the Information Warfare fight, readers are advised to review the Dhillon and Smith article cited later in these footnotes.

[41] The JTF-CNO has organic law enforcement representatives from DOD agencies Naval Criminal Investigative Service (NCIS), Army Criminal Investigative Division (CID), and Air Force Office of Special Investigations (AFOSI), while investigations may also involve other federal and local agencies).

appropriate intelligence or diplomatic agency, such as the CIA or the State Department. If the matter is serious enough, military contingencies may be planned.[42]

The debate revolving around the legal implications of information warfare generally do not include issues related to CND. The right for a nation to employ defensive measures to protect itself is specifically stated in Article 51 of the United Nations charter; although few of the founders of the United Nations could have envisioned the right of self-defense would one day extend to an unseen world of electrons moving about the globe. It is in the interest of the US to ensure that international law and custom support actions taken to neutralize these threats. This includes those treaties relating to the use of space and international telecommunications as well as domestic statutes.[43]

The initial legal difficulty is identification. How will organizations determine if a criminal act (the act of an individual or group in violation of criminal law) or an act of war (the act of a nation in violation of international law) has been committed? The complexity of computer code and the tendency of software to contain errors may also result in innocent malfunctions being mistaken for criminal or terrorist activity.[44] Furthermore, even when incidents can be attributed to a deliberate action, attribution is

[42] Major David J. DiCenso, USAF (Ret), "IW Cyberlaw: The Legal Issues of Information Warfare," *Airpower Journal* (Summer 1999), 86.

[43] James P. Terry, "The Lawfulness of Attacking Computer Network in Armed Conflict and In Self-Defense in Periods Short of Armed Conflict: What are the Targeting Constraints?," *Armed Forces Law Review*, Vol 169 (September 2001), 87-89.

[44] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law, online edition (Washington DC: National Defense University Press, 2001), URL: <www.dodccrp.org/iwilindex.htm>, accessed 23 January 2002.

still an issue of paramount concern. For example, in Moonlight Maze, the fact that the computers used were in Russian government offices did not necessarily prove that the Russian government sponsored the intrusions. It was equally possible that one or more employees were using government computers without the knowledge of their superiors and were not part of an officially sanctioned plan. Unlike "kinetic" attacks (physical attacks such as those using bombs or bullets), there are often few *reliable* indicators that aid in attribution. Without this proof of origin and intent, international cooperation for extradition or subsequent punishment by other nations of offenders becomes difficult and groups that may pose a cyber-threat to the U.S. military can protect their plausible deniability.[45]

A second legal issue is US justification of retaliatory acts. In recent years, US action has typically been preceded by a flurry of activity designed to develop international consensus and to validate such military action under Article 51 of the UN Charter.[46] Whether the US is willing to undertake "kinetic" (military) action because of computer attack is an unanswered question. Another unclear issue is whether computer attack and kinetic proportional response can be correlated. Does the induced crash of an electrical grid control system, which results in no deaths, warrant a cruise missile attack

[45] Greenberg, Goodman, Soo Hoo. The authors include an extended discussion of the difficulties in prosecuting or extraditing individuals based on current international law. For example, French courts often refuse to extradite individuals for the sole purpose of punishing the offender for laws committed in another country. In other words, a murderer may be extradited, because murder is also a French crime. However, French extradition of an individual for a crime that is only a crime in the United States would be unlikely. It is significant to note that the US (as well as most other Western nations) has responded in a similar manner.

[46] United Nations General Assembly. *Charter of the United Nations*. First session. 26 June 1945. Article 51 has been referenced numerous times by the US to justify action in the wars including Kosovo, Iraq and Afghanistan. In part, Article 51 recognizes the right of "…individual or collective self-defense if an armed

response? What if intensive care patients were to die because of such an attack or perhaps aircraft were to crash because air control systems are disrupted? For now, there is no scale to consult and international law is undefined. Resolution of this issue awaits international cooperation and legal agreements.

A third legal issue for consideration is that the rapid pace of technology has left legal systems around the globe trying to catch up to the technology. Perhaps due to the perceived threat to the nation's critical infrastructure, the US government has moved quickly to outlaw illegal activity that occurs within US national boundaries (see Figure 5) and to develop a series of precedents for protecting information infrastructure. Some observers, including the legal scholar Mark Shulman, have judged the collection of new US federal laws related to cyberspace to be the best in the world.[47] But some other states have not been as quick to realize that the Internet does not respect territorial boundaries and that countries whose laws are antiquated will experience difficulty in prosecuting hackers or more serious criminals. In one of the most publicized examples, the Filipino creator of the "I LOVEYOU" virus could not be prosecuted under Philippine laws that existed at the time (May 2000) he promulgated it.[48] The Philippines, like most second and third world nations, did not have any reference in their legal codes specifically criminalizing promulgation of destructive computer code. Moreover, where there are laws pertaining to cyberspace, most are primarily concentrated on issues of copyright

attack occurs against a Member of the United Nations…" In a cyberspace environment, it may be difficult to convince other nations that it is acceptable to classify computer attacks as armed conflict.

[47] Mark Russell Shuman, *Legal Constraints on Information Warfare* (Maxwell Air Force Base, Alabama: Air University Press, 1999), 8-9.

[48] "'Love bug' prompts new Philippine Law," *USA Today*, 14 June 2000, URL: <www.usatoday.com/life/cyber/tech/cti095.htm> Accessed 27 January 2002.

infringement, freedom of speech, and privacy rather than issues related to war. Until the community of nations comes together to agree on legal sanctions, law enforcement agencies will continue be hampered.

US Law and Cyberspace		
Law	**Impact**	**Penalty**
Computer Fraud and Abuse Act (Primary US Hacker Law). Passed into law October 16, 1986.	- Prohibits cyberspace fraud (U.S.C § 1029) - Details crimes of computer espionage - Prohibits unauthorized access to computer based financial records - Criminalizes unauthorized access to US government computers - Established criminal cyber-trespass law - Prohibits trafficking in computer passwords	Punishment varies according to nature of crime. Maximum penalty: Fine and/or 20 years imprisonment
Wiretap Act. Passed into law January 5, 1999	U.S.C §1030. Makes it unlawful to intentionally intercept, use, or disclose or use to intercept use, or disclose any wire, oral or electronic communication. Notable exceptions include systems administrators with consent of user (hence the notice most network users receive upon login that says use of the system constitutes consent to monitor), and court order.	Punishment varies according to circumstances. Maximum penalty: Fine and/or imprisonment for not more than ten years for initial offense. Up to twenty years for subsequent offense.

Table 2: US Law and Cyberspace. Sources: Mark Russell Shulman, *Legal Constraints on Information Warfare* (Maxwell Air Force Base; Air University Press, 1999), 8-9. *Title 18, U.S.C §1029 and §1030*.

A fourth problem is the domestic and international legal constraints that must be addressed as information warfare increases in importance and significance. Among the most interesting topics, are those related to the Fourth Amendment to the constitution, the Foreign Intelligence Surveillance Act (FISA), the Posse Comitatus Act, and issues related to the Law of Armed Conflict (LOAC).

The Fourth Amendment states: "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[49] Since CND and CNA activities may involve probes and scans of private computers from which attacks may originate, the Fourth Amendment would seem to provide protection to computer attackers (under the rubrics of protected places and things or probable cause). However, although U.S. courts have generally held that the Fourth Amendment protects information on computers, some court decisions have noted that this protection is not absolute when applied to cyberspace, particularly where there is a diminished expectation of privacy.[50] Users of e-mail and Internet users do not have the same expectation of privacy in cyberspace that users of the postal system, for example, can expect.

This is not simply an academic or legal debate for policy makers. The determination of where constitutional rights begin and end in cyberspace will determine

[49] U.S. Constitution, Amendment IV

[50] Joginder S. Dhillon and Robert I. Smith, "Defensive Information operations and Domestic Law: Limitations on government investigative techniques," *The Air Force Law Review* 50, (2001), 135-174.

what activities will require court approval to be conducted. This means or at least implies that certain activities may be protected, thereby giving a potential attacker refuge from discovery and/or prosecution. Law enforcement agencies may find that suspects are able to hide behind a constitutional shield and avoid prosecution, and military strategists may discover that the enemy in cyberspace is nearly impossible to trace and identify with a high level of confidence.

Nevertheless, where there exists a diminished expectation of privacy, the Supreme Court has recognized that in certain circumstances or where "special needs" exist, warrant less searches may be made. For example, Dhillon and Smith theorize that in order to ascertain the identity of a network intruder into a government system, it may be necessary to authorize a special needs exception. In their words, "if the government has a reasonable suspicion unauthorized users are attempting to gain access to critical infrastructures, a limited special needs exception may be appropriate, particularly if the action taken are relatively *unintrusive* and for *limited duration."*[51] Clearly, U.S. domestic law needs to reflect the changing technological landscape.

No example was more indicative of the way in which U.S. domestic law has lagged behind the growth of cyberspace than that of the Foreign Intelligence Surveillance Act (FISA). Passed during the Ford administration and in the wake of Watergate excesses of power, Congress sought to regulate legitimate electronic surveillance while limiting the potential abuses of presidential-directed warrant less surveillance operations against political enemies. Essentially, the act divided potential surveillance subjects into

[51] Dhillon and Smith, 147. (emphasis added)

two camps: U.S. citizens, including lawful resident aliens and companies incorporated in the U.S., and agents of foreign powers or foreign-based groups based in the U.S. who are not protected by U.S. constitutional guarantees.[52] The U.S. citizens/lawful aliens are protected to an extent against electronic surveillance, although surveillance can be authorized via court order, but the agents of foreign powers or foreign-based groups have no such protection.

Designed in a world where the masses had no access to computers, FISA was not something that generated much in the way of comment or outcry. However, in the more than twenty years since the act took effect, computers have become widespread, and hacking incidents and computer intrusions have grown just as quickly. For years, U.S. based hackers were essentially protected by the FISA which prohibited issuance of electronic surveillance orders unless probable cause could be shown that the subject of the surveillance might be an agent of a foreign power or working in concert with a foreign state. Since most of the subjects did not have any obvious ties to a foreign government, an offender was usually only caught after he/she had caused significant damage. By far, the more likely outcome was that the hacker simply disappeared back into anonymity. New laws, including the passage of the PATRIOT Act have closed the loopholes that existed before the terrorist attacks on America.[53] However, it is logical to

[52] Dhillon and Smith, 160-165.

[53] *Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001*, H.R. 3162, S. 1510, Public Law 107-56. This new law provides less legal maneuvering room for hackers/attackers to hide themselves. Penalties for cyber-trespassing and related cyber crimes cyber crimes have been increased and the threshold for granting subpoenas to obtain electronic records in investigations is lowered. The law was passed over the strenuous objections of civil libertarians and organizations such as the American Civil Liberties Union. Cited hereafter as PATRIOT Act of 2001.

assume that some foreign power may have taken advantage of this loophole and was able to avoid detection and was protected by the FISA.

The Posse Comitatus Act also hampers organizations such as the JTF-CNO and other military organizations in their efforts. The act was signed into law in 1878 in response to Southern complaints of harassment by Federal troops used for law enforcement during Reconstruction; this law prohibits the use of the armed forces to execute the laws of the U.S. against its citizens. [54] Special accommodation has been made for allowing Congress and the President to authorize the military to conduct some operations, such as drug interdiction, but the act has remained largely untouched since its passing and there is little political will to change its wording. [55]

The Posse Comitatus Act had the practical effect of preventing active military involvement in tracking down intruders and hackers in DOD networks. It is just for that reason that the JTF-CNO and similar organizations have now integrated law enforcement personnel within their organization to handle investigative, surveillance, and arrest functions in much the same way as the Coast Guard performs law enforcement function while assigned to a Navy boarding party in drug operations. This law enforcement component is equally valuable when trying to identify and apprehend offenders across

[54] Title 18, U.S. Code, Section 1385.

[55] Bonnie Baker, "*The Origins of the Posse Comitatus*," Aerospace Power Chronicles, November 1999. Online version available at URL: http://www.airpower.maxwell.af.mil/airchronicles/cc/baker1.html. In the last century, Presidential authority was used on rare occasions to negate Posse Comitatus. Examples include the use of the Army under General Douglas MacArthur to break up World War I demonstrators during the Washington "Bonus March" in March 1932 and President Harry Truman's threatened the use of the Army to break a railroad strike in May 1946. Curiously, the act only applies directly to the U. S. Army and Coast Guard.

international borders. At present, only when the “bad guy” is a country or military force of a country can the CNA trigger be pulled.

Finally, there is the issue of CNA and the Law of Armed Conflict. Based on the Geneva Conventions of 1949 and 1977, the agreements from these conventions form a rulebook for modern warfare.[56] These rules seek to protect civilian populations, outlaw discriminate attacks on populated cities, and, in general, seek to set boundaries for the conduct of war.

However, these boundaries may not be useful in the conduct of CNA. For example, perfidy is outlawed.[57] There are also remnants of a chivalric past that remain in most modern militaries that help mitigate the violence of warfare. Societal and legal injunctions, for example, reward warriors for preventing casualties to women and children and ostracize at a minimum those who are involved in atrocities.

One may argue that the Law of Armed Conflict and chivalric notions can exist because the opponent can be identified and their status determined. However, on the modern cyber-battlefield, there is no way to determine for sure who the opponent may be. Is the hacker who is trying to access classified information about troop movements in time of war a curious teenager or a professional solder? The answer will determine the acceptable response to the hacking activity. If excessive force is applied against what turns out to be a relatively harmless teenager (perhaps a U.S. unit decides to permanently take out the troublesome spy with a kinetic attack), it is not a great leap in logic to

[56] Schulman, 11.

[57] Perfidy is unlawful trickery of the opposition. Examples include faking surrender to gain an advantage; pretending to be a noncombatant or pretending to be a neutral party by wearing the uniform or

conclude that someone in the military command may face charges of killing what the international community may regard as a noncombatant.

Problems can arise from not only the death of people, but also the destruction of protected buildings and facilities. Among the Geneva conventions is the Convention for the Protection of Cultural Property. Included in this category are religious sites, dams and reservoirs, hospitals, and cultural/historic sites.[58] All are protected in wartime so long as they are not used in a manner to shelter enemy military capability, or overtly support or promote the war effort. Would the U.S. violate this convention if its military force disrupted an electrical power grid and the result was patients dying who depended on electrical power to run their life support equipment? What if farmland flooded to such a degree that crops were ruined? The U.S. could possibly be accused of violating these international agreements, as part of an enemy's information war against this country.

An opposing argument explored by Schulman is the belief that information operations, including CNA can ultimately save lives. By minimizing or eliminating the possibility of civilian casualties and damage to civilian infrastructure, some military ethicists argue that the sooner IW tactics are employed, the less likely permanent damage will linger in an enemy's country, and the less infrastructure will need to be rebuilt. Taken to its logical extreme, IW may eliminate the need to recreate the horrors of Hiroshima and Nagasaki, Dresden and Cologne.

Yet, despite the tantalizing possibilities of waging a "surgical" CNA/IW war, there are still very complicated issues to resolve. For instance, the same Protocol I of the

identification of a neutral party, such as the UN. However, this does not prohibit military forces from using deception, misinformation, or other means to mislead the enemy. Schulman, 14.

Geneva Convention states that combatants must distinguish themselves from the civilian population. The intent is to distinguish who is a combatant and therefore a "legal" target, and who is not. When forces operate in the physical world this is relatively easy to do. The military man or woman will usually be in uniform. If they are using a vehicle, the airplane, truck, or tank, it should have markings that identify the country of origin. By separating and clearly identifying military personnel and their infrastructure both become valid targets. However, what happens when those same forces use civilian communications lines (ATT, MCI, etc) to transmit voice or data communications? Does the use of the civilian communications spectrum mean that the communications network is now a legitimate target?

It is apparent that the legal ramifications of information warfare are very complex, far-reaching, and still to be assessed within domestic and international legal forums. Until these issues are resolved, national and armed forces leaders would be wise to tread carefully or risk alienating allies and violating existing international treaties and agreements.

[58] Schulman, 15.

Conclusion

The day may come when warfighters look back on war in the late 20th century with something approaching nostalgia. When that time comes, the warrior may long for the days when the enemy was clearly identified and could be engaged in a definite time and space. While the argument can be made that warfighting in the past 25 years has grown more complicated, information warfare has the potential to become more complex to an exponential degree. It is an area of conflict that is global in scope that touches on every element of national power; it also reaches across civilian, armed forces, law enforcement, and defense boundaries. Although warfare as traditionally known is a complicated business, two factors make information war very different.

The first is that identification of the enemy is extremely difficult, if not impossible. Attacks that originate inside of the United States can be handled via law enforcement and criminal penalties. However, what about those that originate outside of a nation's borders? Does the fact that a hacker attack or criminal intrusion originates in another country mean that that country has sponsored the action? Of course not, and that is part of the dilemma. Furthermore, sophisticated hackers possess the ability to "spoof" (impersonate) individuals online to such a degree that attribution with a high degree of confidence is difficult. But, depending on the context in which these intrusions and attacks occur, the United States may be compelled to respond with "kinetic" (bombs, bullets, etc.) or CNA assets. This is particularly true if the action is evaluated as a serious terrorist threat to the civilian or armed forces critical infrastructure.

However, would such an action be considered an appropriate use of force under international law? International case law is murky and ill defined. Although nations have the inherent right of self-defense, that right was recognized during a time that did not envision cyber-warfare. Whether a cruise missile attack or the disruption of a nation's communication or electrical power infrastructure is an appropriate response to a denial or service attack is questionable. The severities of unintended consequences from defensive (or offensive) actions are difficult to determine. Will disruption of another country's infrastructure result in the deaths of innocents? Will the global world community support the United States to a certain threshold and then no further? Currently, there is no scale of moral equivalency to which the armed forces and civilian officials can refer to help them with these decisions. It is no wonder that authorization to employ CNA remains at the highest levels of civilian authority.

The second major difference between conventional war and information war is that the players may be almost anyone who can operate a keyboard. Where an armed forces uniform and identification with a fighting force defined combatants in centuries past, the cyberspace opponents may be anyone from a curious teenager to a technically sophisticated terrorist to a highly educated operator in the employ of a nation state. Furthermore, determining the motivation for that opponent will also be difficult. Is the threat simply an individual criminal intent on robbery? Alternatively, is the attacker on the other end of the connection inspired by patriotism, religious fanaticism, nationalism, ideological commitment, or something else? The answer may dictate whether a response is necessary and the means of the response. Again, for now there is little guidance for staffs and decision makers to follow.

Despite the uncertainty, there are some hopeful signs. After the 11 September 2001 terrorist attacks, there has been a drop in the number of computer intrusions and attacks detected by the JTF-CNO and the NIPC. Some have attributed the decline to increased defensive capability, others to tougher penalties and investigative power via the controversial PATRIOT Act. In the words of U.S. Space Command commander, General Eberhart believes they "are afraid to challenge us in this realm, because they know we're mad, and they're worried about repercussions."[59]

Although some may take heart that organizations such as U.S Space Command are taking the lead in combating cyber-adversaries, this writer would caution that there is room for uncertainty as well as hope. The SPACECOM arm charged with the execution of the CNA/CND mission, the JTF-CNO, is undermanned, underfunded, and faced with a tremendous mission challenge. Imagine having the responsibility for defending *all* DOD computers and computer networks with a budget of less than 20 million dollars and (currently) less than one hundred assigned personnel! It is a huge task that will only grow more difficult over the next decade. One can be hopeful because the JTF-CNO is a pathfinder organization. This implies a larger and more capable organization is expected to evolve at sometime in the future. Meanwhile, as the nation builds and fortifies its cyber defenses, its adversaries will become more sophisticated as will the technology and software they employ. The race for information dominance and information assurance is on, with the US in the lead. The question is how long that lead will last.

[59] Hoffman, "A Surprise: Fewer Cyber-Attacks after 9-11," online article

Appendix A

Acronyms

CERT	Computer Emergency Response Team
CINC	Commander-in-Chief
CNA	Computer Network Attack
CND	Computer Network Defense
DISA	Defense Information Systems Agency
DOD	Department of Defense
GAO	General Accounting Office
GNOSC	Global Network Operations Security Center
JTF-CND	Joint Task Force-Computer Network Defense
JTF-CNO	Joint Task Force-Computer Network Operations
JV 2010	Joint Vision 2010
LOAC	Law of Armed Conflict
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
PATRIOT	Provide Appropriate Tools Required to Intercept and Obstruct Terrorism
PCCIP	President's Commission Critical Infrastructure Protection
PDD	Presidential Decision Directive

Appendix B

CND/CNA Event Timeline

1988 First Internet Virus

1991 GNOSC (Global Network Operations Security Center) established

1993 DOD CERT (Computer Emergency Response Team) established

1996 Executive Order 13010 signed

1997 Joint Vision 2010 published

- Eligible Receiver exercise

- Clinton Administration produces Critical Infrastructure Protection document

1998 Solar Sunrise intrusion detected

- PDD (Presidential Decision Directive) 63 signed

- JTF-CND formed

1999 Moonlight Maze intrusions

2000 USSPACECOM assigned CND mission

- National Infrastructure Protection Plan published

- E-commerce denial of service attacks against EBay and other online vendors

- Joint Vision 2020 published. Decision Superiority one of the main pillars.

2001 JTF-CND changes name to Joint Task Force-Computer Network Operations. USSSPACECOM receives CNA mission and assigns responsibility for execution to JTF-CNO.

Appendix C

A Service Perspective

Upon first examination, the Marine Corps warfighting philosophy might not seem as compatible to waging information warfare as the other services, particularly as information warfare relates to computer network operations. The emphasis on the ability to "shatter the enemy's cohesion through a series of rapid, violent, and unexpected actions that create a turbulent and deteriorating situation with which he cannot cope" seems to focus on the type of combat that comes to mind when one thinks of such battles as Tinian and Inchon.[60] However, such a view is erroneous.

The modern Marine Corps has indeed addressed information operations and has integrated these operations into the Marine Air Ground Task Force (MAGTF) and single battle concepts. Marine Corps information operations are viewed as supporting operations to decisive maneuver warfare. The goal is to "use information to *deny*, *degrade*, *disrupt*, *destroy*, or *influence* an adversary commander's methods, means, or ability to command and control his forces and to *inform* target audiences through informational activities."[61]

[60] U.S. Marine Corps, *FMFM 1: Warfighting* (Washington, DC: GPO, 1989), 61.

[61] Marine Corps Combat Development Command, "Marine Corps Warfare Publication (MCWP) 3-40.4 Information Operations (Coordinating Draft)," URL: http://www.doctrine.usmc.mil/mcwp/view/mcwp3404/mcwp3404.pdf. Accessed 22 March 2002. 5. Hereafter cited as MCWP 3-40.4 Draft.

In much the same way as the other services, the Marine Corps views information warfare as being composed of more than just generic computer network operations. Offensive information operations are broken down into the following methods:

- Operational security (OPSEC)
- Military deception
- Electronic warfare (EW)
- Psychological operations (PSYOP)
- Physical attack/destruction
- Computer network attack.

Defensive information warfare elements include:

- Physical security
- Operation Security (OPSEC)
- Counter-propaganda
- Counter-deception
- Information assurance (IA)
- Electronic protection
- Counter-intelligence
- Computer network defense (CND).[62]

During MAGTF operations, information operations may even become the main effort of an operation.[63]

Significantly, although the Marine Corps recognizes the importance of information warfare in the modern battlespace, it is also realistic about the resources

[62] MCWP 3-40.4 Draft, 5.

[63] MCWP 3-40.4 Draft, 10.

needed to develop a Marine Corps specific capability that can travel with the Marine Expeditionary Force (MEF), the Marine Expeditionary Brigade (MEB), or the Marine Expeditionary Unit (MEU). In the coordinating draft of Marine Corps Warfare Publication 3-40.4, *Information Operations*, commanders are advised not only to just familiarize themselves with the information warfare capabilities, but that they should expect to have access to information warfare tools available via "reachback" to national, CINC, or Joint Task Force (JTF) level assets.[64] The implication is that these capabilities will not be organic to the Marine Corps field units. Whether this is a function of dollars or fighting philosophy is a matter of debate, but an access capability will still be a casualty.

An argument can be made now that the relative small size of the Marine Corps works against itself as it attempts to prepare for CND and CNA-centric operations. As the other services race to establish organizations with a computer network attack or computer network defense orientation, the Marine Corps is struggling to compete for these same types of resources. In addition, while the much publicized 6.9 billion dollar Navy and Marine Corps Intranet program will help the Marine Corps modernize its information technology infrastructure, the focus of these funds will be to enhance productivity, standardize information technology training, and improve data transfer capability.[65] There are few, if any, funds allocated for developing CND or CNA capability.

[64] MCWP 3-40.4 Draft. 6-7.

[65] "Navy-Marine Corps Announce Intranet Contract Award," Assistant Secretary of Defense News Release, 06 Oct 2000, URL: http://www.c3i.osd.mil/ebpublic/NMCI_contract.pdf, accessed 21 March 2002.

In spite of this, the Marine Corps characteristic style of quick and violent operations in land combat may be an advantage. Enemy forces will continue to have less time to target critical network vulnerabilities because of the rapid maneuver warfare ethic; once an adversary is identified, he will have to try to conduct operations against highly mobile targets in the field. The threat may actually be more pronounced for fixed bases and logistical sites that depend more heavily on information technology. It will certainly not be eliminated, as opponents are likely to seek out attractive fixed targets such as fixed headquarters sites, information technology network hubs, supply depots, and similar targets vice the mobile field units such as the MAGTF.

Bibliography

Due do its relative recent identification as a new component of conflict, there is relatively little discussion of information warfare in the literature prior to the late 1980s. Much of what remains from that initial period has been rendered obsolete by sweeping changes in technology. The publications from the military services have proven to be valuable resources in conducting research for this paper.

It is also probably not surprising that since the focus of this paper is computer and computer networks, that the Internet was also a valuable resource. Researchers in the federal government, private industry, and academia now "publish" articles online and nearly every journal of note has an online version that can be accessed anywhere there is Internet access.

Most importantly, the requirement for the researcher to remain vigilant and to use only reputable sources is more challenging in an Internet environment. In conducting research for this work, the author has attempted to rely on sites of prominence and reliability that other researchers can readily access.

Primary Sources

Government Documents

United States. U.S. Constitution, Amendment IV

United States. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets* (Washington DC: GPO, 2001).

United States. Joint Staff, *Joint Vision 2010* (Washington DC: GPO, 1996).

This important document was the "roadmap document" that set a path for the military in the post-Cold War years. The emphasis was on light and adaptable forces that could effectively leverage the technological superiority of the United States in the asymmetric environment that planners expected to face in the early 21st century

United States. Secretary of Defense (William S. Cohen), letter to CINCs, Services and Agencies, subject: "Joint Task Force-Computer Network Defense Charter," 4 December 1998.

This letter sent to the CINCs, Services and Agencies set up the JTF-CND. The goal was to begin addressing the concerns expressed in PDD 63 and other documents. It is somewhat humorous to note the small amount of personnel and funding resources that were allocated in the beginning to secure all DOD computers and computer networks. At its inception, the organization had only 18 military personnel and a miniscule 3.1 million dollar budget. This relatively small commitment of resources is similar to the way in which the military funded other new elements in warfare such as early 20th century aircraft.

United States. United States Congress. United States Code. Posse Comitatus Act of 1878, Title 18, U.S. Code, Section 1385.

United States. United States Congress. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, H.R. 3162, S. 1510, Public Law 107-56.

This little known law signed in October 2001 has had far-reaching impact on the legal landscape of cyberspace. In one fell swoop, its enactment has largely made moot concerns such as the FISA. It has also given increased powers to law enforcement agencies and enabled officials to easily monitor electronic communications in the private and government sectors.

United States Commander-in-Chief Space Command. Letter to Commander, Joint Task Force-Computer Network Defense and others. Subject: "Redesignation of Joint Task Force-Computer Network Defense." 23 March 2001.

U.S. President. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures,* October 1997.

U.S. President. Executive Order 13010, "Critical Infrastructure Protection." 15 July 1996.

U.S. President, Executive Order 13231, "Critical Infrastructure Protection in the Information Age." 16 October 2001. Version referenced from *Federal Register* 66, no 202 (18 October 2001): 53063.

U.S. President, Presidential Decision Directive NSC 63, "Critical Infrastructure Protection." 22 May 1998.

Briefings

Joint Task Force –Computer Network Defense "CINC Decision Brief" briefing presented by JTF-CNO. Colorado Springs, CO, N.P., 28 February 2001.

This brief was presented to CINCUSSPACECOM to ask for his decision to expand the JTF-CND to assume the CNA mission. It is a step by step primer of not only the future goals of the organization, but a history lesson in why there was a need for a JTF-CND and what it had accomplished in its eighteen plus months of existence. Original brief previously unpublished. Briefing document is currently held in Plans Directorate (J-5) of the Joint Task Force-Computer Network Operations (JTF-CNO), which is co-located at the Defense Information Systems Agency (DISA) headquarters in Arlington, VA.

Joint Task Force – Computer Network Operations "CNO Operations Brief" briefing presented by JTF-CNO. Arlington, VA, N.P, May 2001.

This briefing is currently held in Operations Directorate (J-3) of the Joint Task Force-Computer Network Operations (JTF-CNO), which is co-located at the Defense Information Systems Agency (DISA) headquarters in Arlington, VA.

Joint Task Force – Computer Network Operations "JTF-CNO Command Brief", briefing presented by JTF-CNO. Arlington, VA, N.P., 01 November 2001.

This briefing material is currently held in Operations Directorate (J-3) of the Joint Task Force-Computer Network Operations (JTF-CNO), which is co-located at the Defense Information Systems Agency (DISA) headquarters in Arlington, VA.

Bacon, Kenneth H., "DOD News Briefing with Assistant Secretary of Defense (Public Affairs)," 16 April 1998. URL: <http://www.defenselink.mil/news/Apr1998/t04161996_t0416asd.html>, Accessed 14 January 2002

Secondary Sources

Books

Although books that focus on computer warfare, information operations and related subjects are appearing with increasing frequency, there is still a dearth of literature on these subjects. Many of the books available in libraries are products of the late 1980's and early 1990's. Technology has rendered much of what was forecast in these early works obsolete. Below are more recent works that are still relevant for current IW issues.

Shuman, Mark Russell. Legal *Constraints on Information Warfare*. Maxwell Air Force Base, Alabama: Air University Press, 1999.

A superb, compact work that raises as many questions as it answers about the legal problems associated with all forms of Information Warfare.

U.S. Marine Corps, FMFM 1: Warfighting. Washington, DC: GPO, 1989, 61.

Periodicals

Periodicals are a richer source of research material on IW. In addition to the items listed, readers may find several university and professional military education institutions have produced articles on this subject. The mainstream media has focused on the more sensational aspects of the issue and the serious reader should investigate more scholarly and technical journals for a less sensational but more informative perspective. Of particular interest are various legal journals available in most research institutions. The legal community has recognized the law is lagging on this issue, and it is interesting to witness the development of domestic and international precedents on the topic.

Baker, Bonnie, “The Origins of the Posse Comitatus,” *Aerospace Power Chronicles*, (November 1999).

Dhillon, Joginder S. and Robert I. Smith, “Defensive Information operations and Domestic Law: Limitations on government investigative techniques,” *The Air Force Law Review* 50, (2001).

DiCenso, Maj David J., USAF (Ret), “IW Cyberlaw: The Legal Issues of Information Warfare,” *Airpower Journal* (Summer 1999).

Fulghum, David A. and Robert Wall “Combat-Proven Infowar Remains Underfunded,” *Aviation Week & Space Technology*, 26 February 2001.

Gertz, Bill, “Eligible Receiver,” *Washington Times*, 16 April 1998, Final Ed.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo, Information *Warfare and International Law*, online edition (Washington DC: National Defense University Press, 2001), URL: <www.dodccrp.org/iwilindex.htm>, accessed 23 January 2002.

“’Love bug’ prompts new Philippine Law,” *USA Today*, 14 June 2000, URL: <www.usatoday.com/life/cyber/tech/cti095.htm> Accessed 27 January 2002.

Sbrocco, Ed, Tom Ward, and Chris Baden, "Cyber Terror – Potential for Mass Effect," *IA (Information Assurance) Newsletter* 4, no. 4 (Winter 2001/2002): 6.

Terry, James P. "The Lawfulness of Attacking Computer Network in Armed Conflict and In Self-Defense in Periods Short of Armed Conflict: What are the Targeting Constraints?" *Armed Forces Law Review* Vol 169 (September 2001)

Other Documents

By far, the most up to date information on Information Warfare, CND, and CNA is found on the Internet. Much of the research that will later appear in periodical or book form appears first on the World Wide Web. However, this accessibility comes at a price. Researchers must be particularly vigilant to ensure that reference material is the result of reputable scholarship and not simply an opinion gleaned from someone's personal website. Researchers are advised to concentrate their initial searches to online versions of reputable "hard-copy" journals and branch out as needed. Researchers with access to the SIPRNET will also find a wealth of classified material on several government sites, including USSPACECOM's.

"Eligible Receiver Exercise Shows Vulnerability," Infowar, 22 December 1997, URL: <http://www.infowar.com/civil_de/civil_022698b.html-ssi>. Accessed 15 January 2002.

Hoffman, Lisa, "A Surprise: Fewer Cyber-Attacks after 9-11," Scripps *Howard News Service* available at URL: <www.knowstudio.com/shns/story.cfm?pk-CYBERSPACE-01-25-02&CAT-II>, accessed 26 January 2002.

Key, Virginia, “What is Solar Sunrise?,” URL: <www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm>, Date unknown. Accessed on 13 January 2002.

Kimery, Anthony. “Moonlight Maze,” Infowar, 3 December 1999, URL: <http://www.infowar.com/class_2/99/class2_120399b_J.shtml.> Accessed 14 January 2002.

Liang, Qiao and Wang Xiangsui, Unrestricted Warfare (Beijing, China: PLA Literature and Arts Publishing House, 1999), 145-146. A complete text available at: URL: <http://www.terrorism.com/documents/unrestricted.pdf>. Accessed 30 December 2001.

Tompkins, Michael, “Computer Network Defense at the National Level,” URL: <http://rrsans.org/country/defense.php>, 5 December 2000. Accessed 14 January 2002.

United States. Justice Department (Press Release), “Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers,” found at URL: <http://www.usdoj.gov/criminal/cybercrime/ehudpr.htm>, 18 March 1999. Accessed 10 January 2002.

Wilson, J.R., “Cyberwarfare 101,” Armed forces Information Technology. URL: <www.mit-kmi.com/Archives/5_1_MIT/5_1Art4.cfm>. Accessed 31 December 2001